19th ICCRTS

Title of Paper

Conceptual Architecture for Obtaining Cyber Situational Awareness

Topics:

Cyberspace, Communications, and Information Networks (primary topic)

Modelling and Simulation (alternative topic)

Data, Information, and Knowledge (alternative topic)

Name of Authors

André Ferreira Alves Machado
Instituto Tecnológico de Aeronáutica
São José dos Campos - SP, Brazil
majandre@ita.br
majafam97@gmail.com

Edgar Toshiro Yano
Professor
Instituto Tecnológico de Aeronáutica
São José dos Campos - SP, Brazil

Abstract

Obtaining a battlefield Cyber Situational Awareness is a paramount factor for military operations. Currently, the complexity of a large data network, the heavy flow of information and the speed of military operations, demand from the Command and the Control area a great agility in knowledge management. In this sense, the use of integrated kinetic and cyber simulators can help to identify the needs of the Command and Control and provide situational awareness of operational and cyber environments. Conceptually, we present an architecture that helps to recognize the impacts in the kinetic environment caused by cyber-attacks, as well as present a way to identify vulnerabilities of a data network for a particular military mission. Finally, this architecture can also be used as a combat support tool for military planning by calculating risk of cyber-attacks.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2014		**00-00-2014 to 00-00-2014**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Conceptual Architecture for Obtaining Cyber Situational Awareness	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Technological Institute of Aeronautics,Sao Jose dos Campos - SP, Brazil,**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Presented at the 18th International Command & Control Research & Technology Symposium (ICCRTS) held 16-19 June, 2014 in Alexandria, VA. U.S. Government or Federal Rights License

14. ABSTRACT
Obtaining a battlefield Cyber Situational Awareness is a paramount factor for military operations. Currently, the complexity of a large data network, the heavy flow of information and the speed of military operations, demand from the Command and the Control area a great agility in knowledge management. In this sense, the use of integrated kinetic and cyber simulators can help to identify the needs of the Command and Control and provide situational awareness of operational and cyber environments. Conceptually, we present an architecture that helps to recognize the impacts in the kinetic environment caused by cyber-attacks, as well as present a way to identify vulnerabilities of a data network for a particular military mission. Finally, this architecture can also be used as a combat support tool for military planning by calculating risk of cyber-attacks.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**61**	

1. Introduction

With the growing capability of technological means and, consequently, increasing the speed of military operations, information on the battlefield has become a valuable target for the military officers.

In this context, the Situational Awareness (SA) of modern combat aims to meet the needs of the Command and Control (C2). In order to lead their military organizations, the commander would require concise information about his and the enemy troops. For example: What are the logistical needs? How to carry out an attack? What is the intention of the enemy?

Moreover, the information should also be timely, because important information, that is late, loses its value. This way the agility of C2, in a Military Command Center, influences directly the power combat of a military organization.

Besides the conciseness and timeliness of the information, the information security, for military operations, is essential and, within the context of information security, the study of cybernetics wins profound relevance.

For this reason, a military commander must know the kinetic and cybernetic battlefield. Obtaining Situational Awareness of Cyberspace can produce significant results for these two environments (kinetic and cyber).

However, the cyberspace is profoundly different when compared with the kinetic space. The tools and processes used in achieving Situational Awareness, in the kinetic space, do not work with the cyber environment [1]. Thus, we need appropriate tools to obtain the required knowledge.

Within this cyber context, many works have been presented in the area of intrusion detection to provide Situational Awareness [2, 3 and 4]. However, in the previously cited work, the approaches are not effective when the attacks are unknown (zero-day attack). Other approaches to analyze cyber risk are able to identify the components of a high risk, but say little about which threats have the greatest impact, how attack time affects the business, or what to do when an attack occurs [5].

Other possible approaches use simulators in cyber security [6]. However, the models recently developed are not fully effective, because of complexity in networks or presence of other limitations in the assessment of impacts.

In our previous work [7], we proposed a theoretical Architecture for defending against cyber-attacks in a real military battlefield using cyber and kinetic simulators

parallel. In this work we present the functionalities of the previously proposed Architecture [7].

2. Related Work

To extend our previous research work [7] in terms of functionalities let's start with a quick review of the proposed approach.

The Figure 1 presents an overview of the previously proposed Architecture [7] with minor changes of nomenclature. This figure contains a real environment, which may consist of military Units, Command Posts, Command and Control Centers.

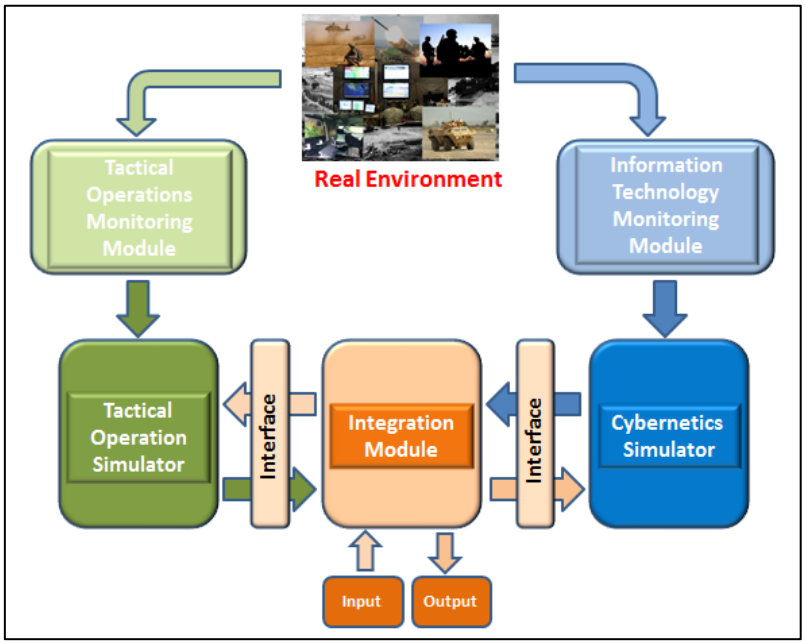


Figure 1 – Architecture [8]

The monitoring module, on the left side, named as Tactical Operations Monitoring Module (TOpM2), performs the capture of tactical information about military actions, i.e.: get data about troop position, logistical and operational needs and other tactical information.

The monitoring module, on the right side, named as Information Technology Monitoring Module (ITM2), performs the reading of the IT infrastructures, from the real environment, capturing the characteristics of network (for example: IT assets, configurations, topology, etc.).

Furthermore, the proposed Architecture uses two simulators: one for military tactics actions and other for cyber operations. The Tactical Operations Simulator (TOpSim) receives tactical data (referring to the real environment) through the TOpM2 and the Cybernetics Simulator (CyberSim) receives IT information through ITM2.

The main purpose for using simulators in the proposed architecture is to build scenarios (kinetic and cybernetic), perform analysis on the scenarios and identify what are the impacts that a scenario can cause on other scenarios.

The TOpSim has the function of simulating the tactical actions that military troops can accomplish. For this, the simulator is dynamically loaded and updated with real information (from TOpM2). When using TOpSim it should be possible to make inferences about military developments in the operational or logistical field.

The CyberSim should perform a detailed analysis on the data transferred from ITM2. Besides the analysis of the network, the CyberSim needs to identify vulnerabilities in operating assets and simulates Denial of Service (DoS) attacks on the discovered vulnerabilities. For the analysis of vulnerabilities, the simulator requires an updated database of vulnerabilities.

Continuing the review of the proposed approach [7], the Figure 1 has two interfaces besides the Integration Module (IM). The interfaces have the task of performing integration between simulators and IM.

Finally, the Integration Module (IM) is responsible to "unite" the kinetic and the cyber environment. For this purpose, it uses the graph structure. The IM has a configuration input, identified, in Figure 1, by the "input box" and a data output, identified by the "output box". The configuration input allows us to program the IM and the output provides reports resulting from the analysis.

The graph is built based on information (about IT assets) obtained from CyberSim, which are identified by the IM and transformed into graph nodes. Edges, that link the nodes of the graph, represent the means of telecommunications used to connect network assets.

After constructing the graphs in IM, the Architecture uses the TOpSim to indicate routes that represents the flow of information, in the graph. If the flow of information has paths (edges and nodes) in the graph, the TOpSim will be informed (by IM) that the task can be executed by the simulator. If there are no possible paths, the IM will not allow the TOpSim simulate the mission.

The consequences of implementing the mission or not (depending on the presence of paths in the graph) in tactical simulator, will result in a sequence of events that will impact the future of military actions. These situations will be simulated in TOpSim.

Finally, in this review, we use some assumptions in the preparation of approach: Every action in logistical or operational field requires a flow of information [9]; The communication system are based on data networks; We have limitations of time, personnel and equipment to protect our data network, which is extensive and complex; Considering the cyber-attack an imminent reality, we need to protect our data network, strengthen the weaknesses and mitigate the impact of a cyber-attack [6].

The details of the possible functionalities of this Architecture are discussed in the next section.

3. Functionalities of the Architecture

With the increasing complexity of data networks, used in military operations, the flow of information becomes large, complex and dynamic. In this sense, questions about which vulnerabilities should be treated first and what the impacts of a cyber-attack, are relevant and need to be answered. With these goals, we will detail the basic functionalities proposed for the Architecture.

3.1 Identification of Vulnerabilities in Relation to Mission

According to some references [10, 11, 12, 13], some cyber simulators already have the functionality to identify vulnerabilities of IT assets in a data network. But, in a large data network, or in a highly dynamic network, there may be from ten to hundreds of vulnerabilities. In such cases, will we have time and resources to solve all the problems, without damaging the progress of a military mission?

In complex data networks, we need to identify which vulnerable assets can disrupt the progress of important military tasks, while under a cyber-attack.

To perform this analysis, using the proposed Architecture, the monitoring modules (ITM2 and TOpM2) retrieves the information about real environment and such information is then used to update simulators (CyberSim and TOpSim). Furthermore, the CyberSim performs the analysis of the data network and identifies potential vulnerabilities. The IM constructs the graph (nodes and edges), based on information from CyberSim (assets, connections and vulnerabilities). After those preparations, the Architecture is ready to identify vulnerabilities in relation to the military mission.

If at this moment, on a real environment, a particular mission is started. This mission (tactical order or logistics request) is identified by TOpM2 that transfers to the TOpSim. The TOpSim sends the information to the IM that unites the information from the two simulators (TOpSim and CyberSim) and checks for paths on the graph.

In the situation shown in Figure 2, we can see that between the node labeled "start" (the sender of the mission) and the node labeled "end" (receiver of the mission), in the mission 1, we have no vulnerable node. However, for mission 2, the path between the node "start" and "end", we have two vulnerable assets (A and B). The same analysis can be made to the Mission 3.

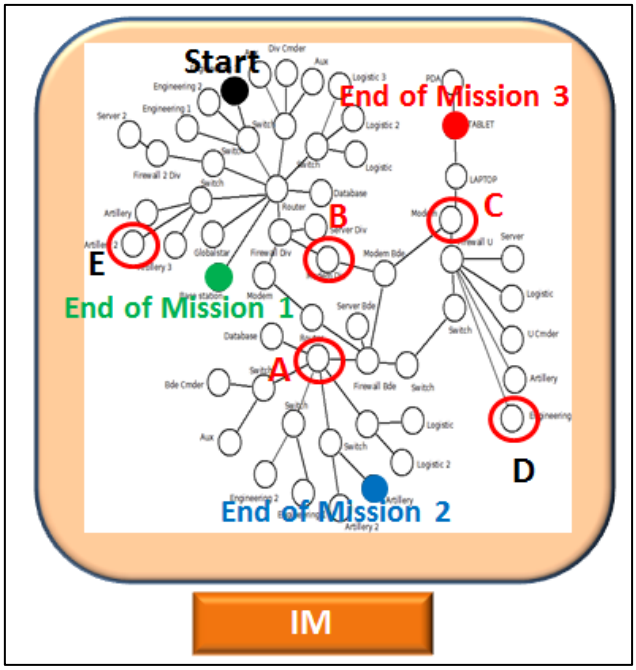


Figure 2 – Path in the Graph [8]

For each mission, identified in Figure 2, the IM makes the path in the graph and identifies, for each possible route, the presence, or not, of vulnerable nodes to a Denial of Service attack.

In the final report (Table 1), we illustrate the status of the three missions with their vulnerable assets. We emphasize that vulnerable assets “D” and “E” (Figure 2) are not related to any present mission and, for this reason, are not presented in the report (Table 1).

Table 1 – Cyber Vulnerabilities Report [8]

Mission	Type	Mission Status	Cyber Vulnerabilities
1	Attack order	Safe	-
2	Artillery Support	Unsafe	Assets A and B
3	Move order	Unsafe	Assets B and C

Using the results of the analysis, a commander can evaluate the situation and identify how many, and which are, the vulnerable assets to a cyber-attack. Thus, he can

decide to correct, or not, the vulnerabilities identified by the Architecture. This decision will depend on the commander based on the importance of the mission.

3.2 Calculation of the Risk

Risk is the combination between the probability of occurrence of a hazardous event and its consequences. The hazard is a real situation that has potential to cause physical damage to persons, systems, equipment or the environment [14]. In this case, according to the reference [14], risk reduction can be achieved by reducing the probability and / or severity of impacts of danger on threatened system.

As we saw earlier, the Architecture can relate the vulnerabilities of IT infrastructure with a specific mission, and missions can be classified, by commanders, according to their importance.

Thus, for the calculation of risk, we can consider that the vulnerabilities, found and classified by CyberSim, are hazardous events to the IT environment and that may cause consequences in the kinetic environment. The degree of importance (priority) of the mission depends directly on the possible consequences.

As an example, in Table 2, we can see that the Mission 1 has more risk than Mission 2 because, although both have the same vulnerability in the asset "A", are different priorities, which impacts the final risk.

Table 2 – Calculus of the Risk [8]

Mission		Vulnerabilities		Risk
Number	Priority	Assets	Occurrence	
1	High	A	75%	Medium
2	Medium	A	75%	Low
3	High	A	75%	High
		C	25%	
4	Very high	-	-	Very low

Comparing the Mission 3 with the Mission 1 (which have the same priority and the same vulnerability in asset "A") verify that the Mission 3 has higher risk, because it has more vulnerability (asset "A" plus "C").

For Mission 4, the Architecture has not identified any asset that has vulnerability to DoS attack and, for this reason, has no probability of occurrence. However, because it is a mission of the highest priority, admits a "very low" risk.

We emphasize that Table 2 has an illustrative purpose to the concept of risk calculation. However, for the calculation (using Equation 1), numerical values should be referred to the priority of mission.

Risk = Priority of Mission x Probability of Hazard (1)

To calculate the probability of the hazard, if exist more than one vulnerability for a mission, they will be considered as mutually exclusive events. That is, the probability should be added (Equation 2).

P (A U B) = P(A) + P(B) (2)

The value of the probability of hazards, i.e. the vulnerabilities found, is the responsibility of CyberSim that need to assign a metric for this determination.

The risk calculation can assist commanders in decision making and planning, as discussed below.

3.3 Identification of Impacts of a Cyber Attack

Identifying the impacts of a cyber-attack requires an understanding of both environments involved (kinetic and cyber). In this sense, the monitoring modules have great importance because it is through them that we get information from these two environments.

The identification of the impact depends on the power of simulation of TOpSim and simulation time. The impact of a cyber-attack on a single computer can propagate over time and influence the functioning of a whole system that, in turn, can impact the military maneuver. That is, computers on DoS attack may, immediately, do not result in any prejudice to a mission, but overtime can cause disastrous consequences.

For the identification of impacts, we will use the Architecture as follows. First, the monitoring modules (TOpM2 and ITM2) are updated with the real environment and pass the data obtained to the simulators (TOpSim and CyberSim). Following, the CyberSim transfers the information about existing assets in the data network to IM, that builds the graph (Figure 3). After this activity, the CyberSim identifies vulnerabilities in data network (Figure 3) and stores this information explained as in the following steps.

Missions (order and request for assistance) are conducted in real environment (Figure 3) and transferred to TOpSim through the TOpM2. The TOpSim transfers data about missions (transmitter and receiver) to IM that identifies, in the graph, the nodes "start" and "end". Before the path in the graph is started, the IM receives information about the vulnerabilities, identified by CyberSim, and performs the "attack" on the respective graph node (Figure 3).

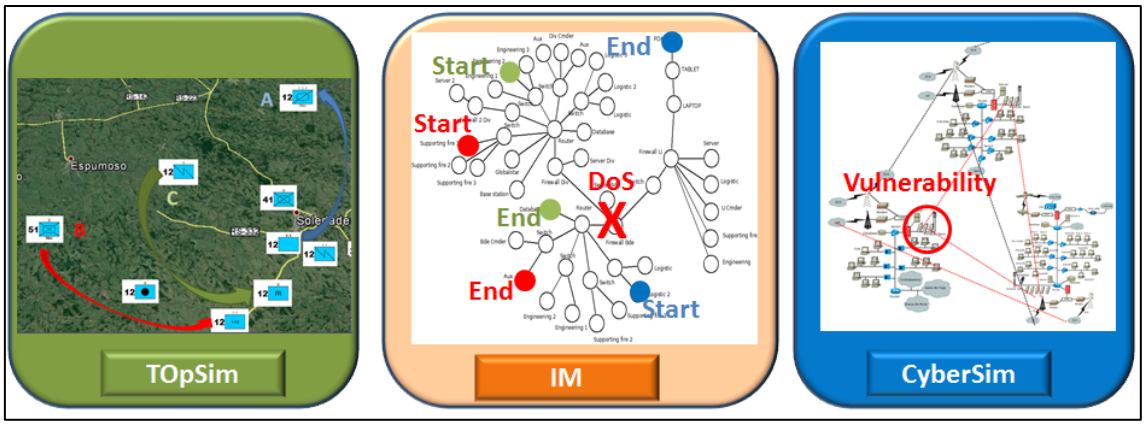


Figure 3 - Graph identified and attacked [8]

If the mission, at some point, suffer the impact of the attack carried out, this information is recorded in IM. If the attack was successful (interrupted the path in the graph), two simulations are made in TOpSim. The first one, containing the mission without attack and the second one, with a successful attack. In addition, the report may contain a simulation time scale, where we can identify the evolution of the impacts on the mission.

Table 3 – Report of the Impact of a Cyber-Attack in Mission [8]

Impact	Mission with efficient attack	Mission without attack
After 1 hour	Unit A at “x” position	Unit A at “x” position
	Unit B requests fuel	Unit B requests fuel
	Unit C request support of engineering	Unit C request support of engineering
After 6 hour	Unit A at “x” position	Unit A at “y” position
	Unit B without fuel (stopped)	Unit B receiving fuel
	Unit C waiting for engineering support	Unit C receiving engineering support
After 24 hour	Unit A at “x” position	Unit A at “z” position
	Unit B destroyed	Unit B on the move
	Unit C waiting for engineering support	Unit C attacks and destroys the enemy

As we can find in Table 3, in the first few moments after the cyber-attack the kinetic effects in the environment are difficult to be perceived, because the only consequence was the interruption of a mission (sending order or request for support). But, over time this lack of communication can result into other impacts. For example, the "A" Unit that should be in the "z" position after 24hours, but it is still in the initial position "x", because it did not receive the order of displacement. The "B" Unit, which requested fuel, stopped because it did not receive the support and is destroyed by the enemy. And, as a last impact, the "C" Unit fails to destroy the enemy, because it did not receive the support of engineering.

Naturally, the effects of a cyber-attack will not propagate indefinitely. The spread of impacts will depend on the reaction time of the element that issued the mission. That is, the time required to identify that his mission is not responded (attacked). Moreover, after the sender identifies that his mission was attacked, he needs to know where the attack occurred, in order to resolve the problem. Otherwise, any other mission (replacing the first) can also be attacked in the same location (vulnerable assets). Therefore, we need to get the Cyber Situational Awareness in order to perform military planning.

3.4 Mission Planning

In planning a military mission, many decisions can be taken. In this study, we will focus on the movement of military troops. This type of mission influences the positioning of Units on the battlefield.

For our approach we focus on the data network that supports the military actions. When we change the position of a military Unit, we are indirectly changing the topology of the data network that supports the information flow of the missions [8].

Each military organization has their data network and when the organization moves carries the entire IT infrastructure. Internally (in relation to an organization) the infrastructure may not modify, but in relation to the whole network (involving all other organizations) changes will certainly occur. Connections can be cut and several others can be created.

Consequently, these changes in connections can include or exclude a set of assets in a data network. According to [6], when new assets are added or removed from a network, the network vulnerabilities also change. And particularly in our approach, these changes on the network influence the construction of the graphs. Thus, possible paths that exist in the graph may disappear and others may also emerge.

Using the Architecture for planning, we do not need the monitoring modules (TOpM2 and ITM2) because updates from real environment, at this time, will not be considered (Figure 4).

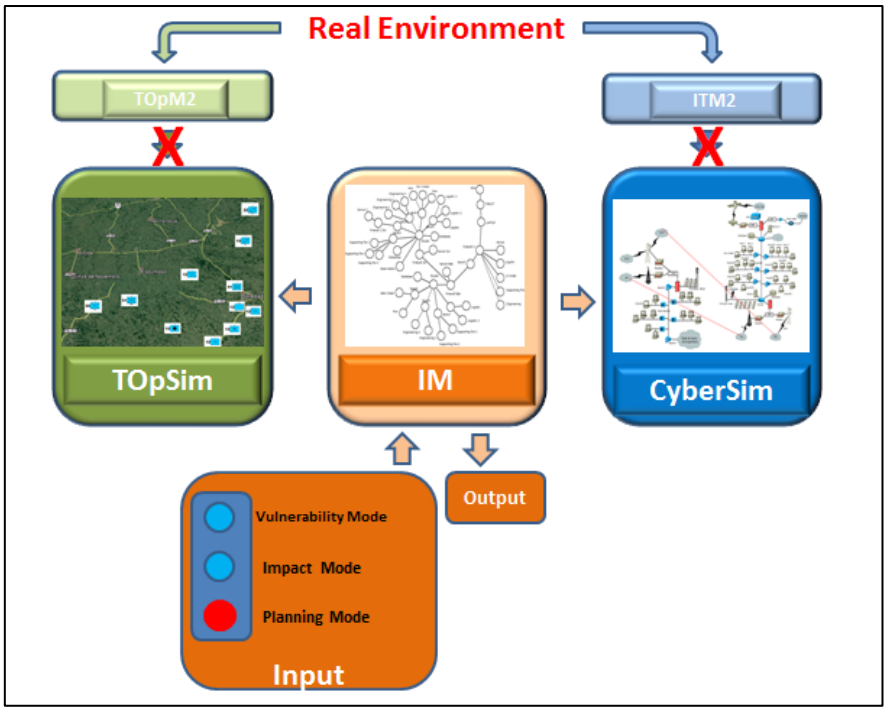


Figure 4 - Architecture in Planning Mode [8]

Tactical planning is done by the military directly in TOpSim. As well as, military personal responsible for IT can update the CyberSim based on tactical updates made in TOpSim (Figure 5).

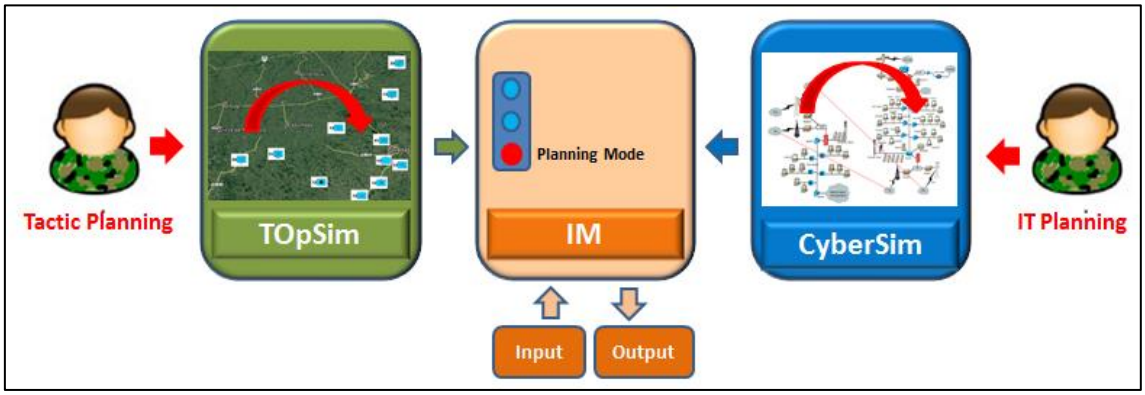


Figure 5 - Tactical and IT Planning [8]

After planning (tactical and IT), the CyberSim analyzes the new data network, identifies new vulnerabilities and sends the updated information to the IM, which constructs a new graph.

In TOpSim, planners identify the most important tasks and initiate the evaluation process. Again, the IM receives information from simulators (TOpSim and CyberSim) finds the paths in the graph (with all possible attacks) and issues a final report.

Table 4 – Plan Report [8]

Mission	Priority	Planning	Vulnerabilities		Risk	
			Before the planning	After planning	Before the planning	After planning
1	High	Alfa	A	A, B and C	Medium	Very high
2	Medium	Alfa	A, B and C.	A and B	High	Medium
3	Low	Alfa	Not identify	A and D	Very low	Low
1	High	Beta	A	Not identify	Medium	Low
2	Medium	Beta	A, B and C	A	High	Low
3	Low	Beta	Not identify	C	Very low	Low

Comparing the results of the report, a commander may decide not to do the planning "Alpha" because it increased the chances of a cyber-attack in mission 1 (very high risk). However, the commander may decide to carry out planning "Beta" because it improves the security level of the most important missions (1 and 2). Moreover, with this report, the commander can identify the problems in the mission 3 (vulnerability in asset C).

The intent of the planning mode is to perform all the planned simulations and check the results (impacts) of the changes, even before they are carried out in the real environment avoiding loss of time, material and lives.

4. Assessment of the Architecture

The proposed architecture was not implemented by the time of the submission. However, some simulations were done for conceptual assessment of the main module of the architecture.

In the general context of the proposed approach, the main module is the Integration Module (IM) because it is through this module that the integration of environment (kinetic and cyber) can be realized.

For the integration of the environments, IM uses the graph structure for representing real world environment (kinetic and cyber). The graph structure should be dynamically constructed using data from cyber environment and dynamically analyzed (if exist path between two nodes) using data from kinetic environment.

Therefore, we propose the use of Java Universal Network Graph (JUNG) for necessary implementation (construction and analysis of graphs) of the IM. Which in turn will help us to realize the evaluation of the approach. JUNG is an open-source library that provides languages to model analyze and visualize data that can be represented using graphs [15].

All tests were performed on a desktop Intel (R) Core (TM) 2 Duo CPU, 4 GB of RAM and 32-bit of operating system. The development environment used was Eclipse.

4.1 Construction of the Graph

To enable the generation of large graphs, we use the algorithm to randomly generated graphs called *random.EppsteinPowerLawGenerator*.

To determine the size of the graph, we need to know how many IT assets exist in the real environment and, while also consequently, in CyberSim. However, this amount varies with the situation, the type of units used, and the military mission. For this reason, in order to perform assessment, we estimate this quantity.

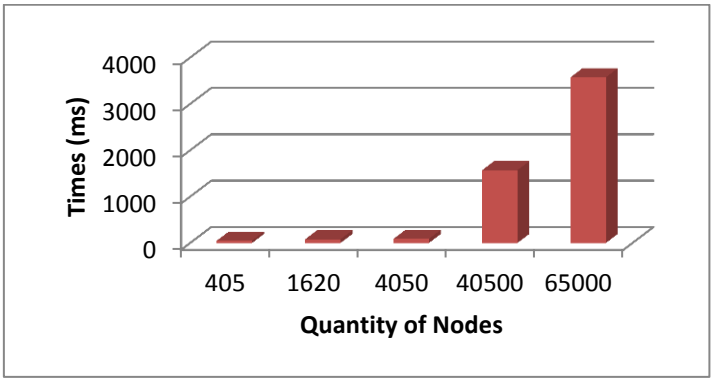
To obtain the average processing time, 30 iterations for each quantity of estimated node were performed.

Thus, for the first assessment, considering that the CyberSim has 405 active, the algorithm needed 49ms (milliseconds) to build a graph with 405 nodes and 500 edges.

Continuing this assessment, to an estimated of 1,620 assets, the average time was 79.8ms for the construction of a graph with 1,620 nodes interconnected by 2,000 edges. Following, the algorithm took 90.1 ms to construct a graph with 4,050 nodes connected by 5,000 edges. We needed 1.570ms to create a graph with 40,500 nodes and 50,000 edges. And, finally, we also got the average time of 3.575ms to construct a graph with 65,000 nodes and 80,000 edges.

The final result of the assessment of *random.EppsteinPowerLawGenerator* algorithm can be seen in Graphic 1.

Graphic 1 – Performance Algorithm for the Construction Graph [8]



With this assessment we conclude that it is possible to create large graphs, in a viable time, for the proposed approach. We must now verify that the remaining analyzes are also viable.

4.2 Analysis of Paths in Graph

Continuing with the assessment of IM, we highlight the important requirements to verify the existence of "paths" between two nodes of the graph. For this activity, we can use *DijkstraShortestPath* algorithm, which has the shortest path between two nodes that are previously identified.

For evaluating the performance of *DijkstraShortestPath* algorithm, we use the same size graphs previously estimated.

As the nodes represent the communication devices and the edges represent the communication links between the nodes, which can be present in the real environment in many different numbers and topographies. Thus for the evaluation, we choose random number of nodes and edges.

Figure 6 shows a graph with 405 nodes and 500 edges. Through the Eclipse environment we can view the graph and identify the paths between the nodes.

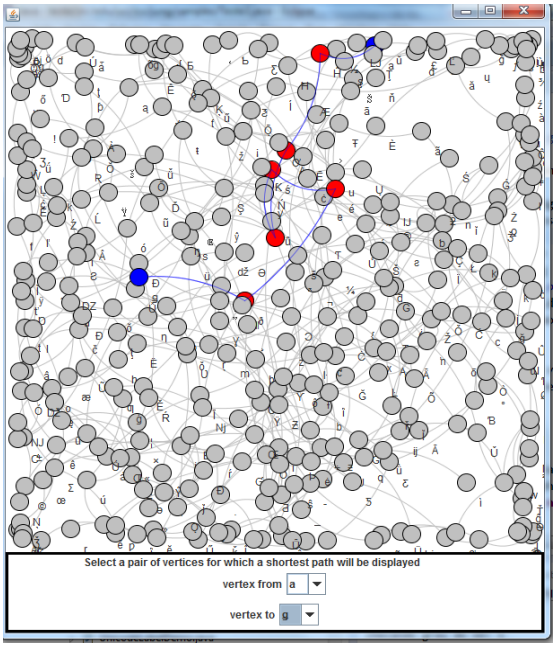


Figure 6 - Path in the graph with 405 nodes [8]

The blue nodes are the “start” and the “end” nodes of the path, the intermediate nodes (of the path) are red, and the blue edges are the paths taken by the algorithm. To generate this path in a graph with 405 nodes, the algorithm took an average of 1.83 ms.

This same assessment procedure was performed for the other graphs. To find the path in the graph with 1,620 nodes (2,000 edges) the algorithm took 4.77 ms. For the graph with 4,050 nodes (5,000 edges) an average of 12ms was necessary. And, for the graph of 40,500 nodes (50,000 edges), the algorithm took 221.5 ms.

Finally, Figure 7 shows the results found for the graph of 65,000 nodes with 80,000 edges. Also presents the Eclipse console where time is presented. In this case, the average time was 229.25 ms.

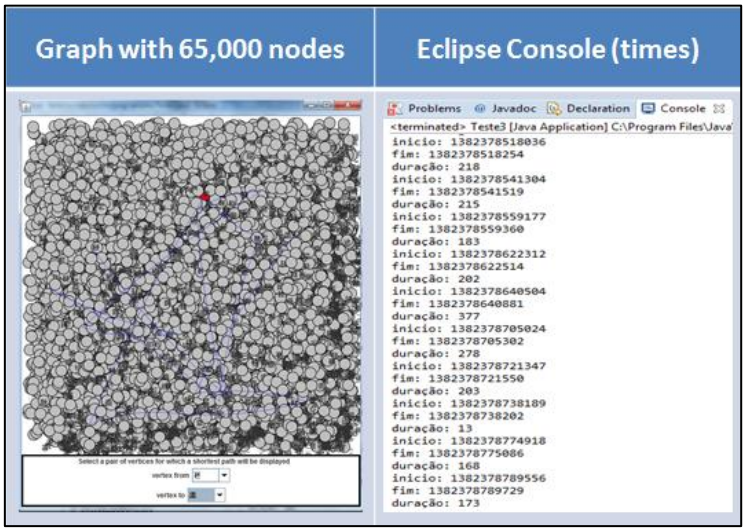
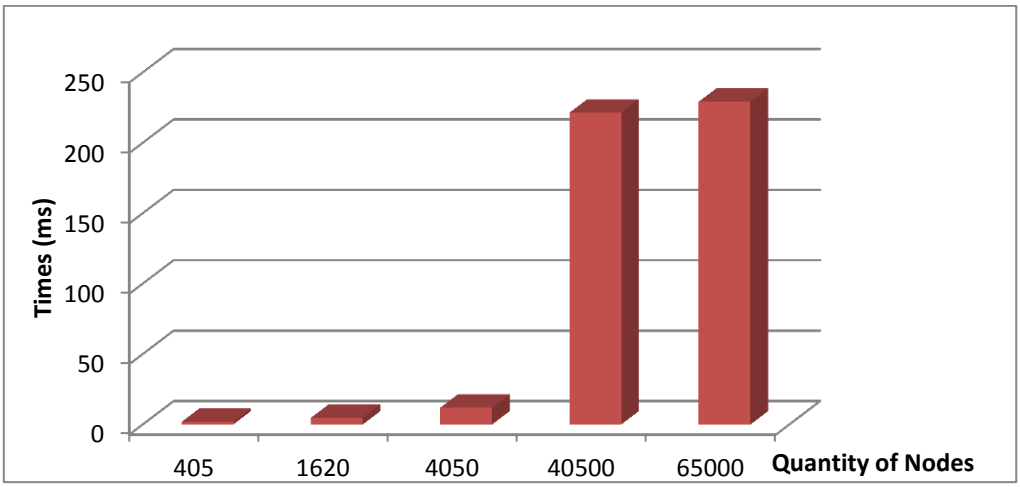


Figure 7 – Graph with 65,000 nodes [8]

To complete the assessment of *DijkstraShortestPath* algorithm, presented in Graphic 2 with the average processing times for each size of graph.

Graphic 2 – Assessment of DijkstraShortestPath Algorithm [8]



5. Final Remarks

This article's main purpose is to extend conceptual understanding about the approach developed in our previous article [7] which is about obtaining the Cyber Situational Awareness of Battlefield.

With this goal, in this article, we present the functionalities expected for Architecture. They are: identify the vulnerabilities of IT assets, in relation to tactical missions; calculating the risk of a mission, considering cyber hazards; identification of impacts of a cyber-attack in the kinetic environment; and the achievement of tactical, cyber and combined planning.

The approach focuses only on the terrestrial military environment and Denial of Service in cybernetic environment. The undocumented attacks (such as zero-day attacks) will not be identified by the proposed Architecture as well as attacks by internal enemies (no vulnerability exploitation) or operator error.

For the assessment of the IM, module which has great relevance to the functionalities of the Architecture, projections were made (about the size of the graph) and evaluations were carried out to estimate the performance of the JUNG framework tasks of construction and identifying paths in the graphs. In both activities, deemed important, the framework achieved a satisfactory performance.

We emphasize that the purpose of the assessment was not to identify a tool or an ideal programming language to perform the analyzes in graph, but rather to verify the feasibility (in terms of processing speed) of the use of graph theory for IM.

As future work, we propose to implement other components of the proposed Architecture and for such future implementation; we also address other types of cyber-attacks, such as the actions of interception, degradation and production of false data in the real environments.

Concluding this work, we believe that Architecture can also be used in other areas. The goal is the same: to identify how a cyber-attack could affect the study area.

References

[1] BARFORD, P; DACIER, M.; DIETTERICH, T. G.; FREDRIKSON, M.; GIFFIN, J.; JAJODIA, S.; JHA, S.; LI, J.; LIU, P.; NING, P.; SONG, D.; STRATER, L.; SWARUP, V.; TADDA, G.; WANG, C.; YEN, J. Advances in Information Security. **Cyber situational awareness**: issues and research. New York: Springer, 2009. (Advances in Information Security, v. 46) ISBN 978-1-4419-0139-2.

[2] DENNING, D. E. An intrusion-detection model. **IEEE Transactions on Software Engineering,** v.13, p. 222-232, 1987.

[3] BASS, T. **Multi sensor data fusion for next generation distributed intrusion detection systems.** IRIS National Symposium on Sensor and Data Fusion. [S.l.: s.n.]. 1999.

[4] SCHNEIER, B. (1999). Attack trees: Modeling security threats. Dr. Dobb's journal. Available: https://www.schneier.com/paper-attacktrees-ddj-ft.html. Accessed: 11 out. 2013.

[5] MUSMAN, S.; TEMIN, A.; TANNER, M.; FOX, D.; PRIDEMORE, B. (2010). Evaluating the Impact of Cyber Attacks on Missions. MITRE Corp, McLean, VA, 22102.

[6] JAJODIA, S.; NOEL, S. Topological vulnerability analysis. In: JAJODIA, S. et al. **Cyber situational awareness**: issues and research. New York: Springer, 2010. p. 139-153. (Advances in Information Security, v. 46)

[7] MACHADO, A; BARRETO, A; YANO, E. Architecture for cyber defense simulator in military applications. In: INTERNATIONAL COMMAND AND CONTROL RESEARCH AND TECHNOLOGY SYMPOSIUM, 18., 2013, Alexandria. **Proceedings...** Alexandria: CCRP, 2013.

[8] MACHADO, A. F. A.; YANO, E. T. Architectural concept of a simulator for cyber situational awareness. 2013. Thesis (Master degree in computer engineering). Instituto Tecnológico de Aeronáutica. São José dos Campos, 2013.

[9] ALBERTS, D. S.; HAYES, R. E. **Understanding command and control**. Washington, D.C.: CCRP Publication Series, 2006. 255 p. ISBN 1-893723-17-8.

[10] SKYBOX SECURITY. Developer´s Guide. Skybox View. Manual.Version 11. 2010.

[11] SCALABLE Network. EXata communications simulation platform. Available: <http://www.scalable-networks.com>. Accessed: 16 jun. 2012.

[12] DECATRON. **Executive project**. Cyberwar operation simulator. Rio de Janeiro. Nov. 2011.

[13] LEEUWEN, V. et al. Cyber Security Analysis Testbed: combining real, emulation, and simulation. In: INTERNATIONAL CARNAHAN CONFERENCE ON SECURITY TECHNOLOGY. **Proceedings…** San Jose: IEEE, 2010.

[14] STOREY, N. **Safety-Critical Computer Systems**. [S.l.]: Prentice-Hall, 1996.

[15] JUNG. Java universal network graph framework. Available: http://jung.sourceforge.net/index.html. Accessed: 10 set. 2013.

19th ICCRTS

Conceptual Architecture for Obtaining Cyber Situational Awareness

Authors:

Maj André Ferreira Alves Machado

Prof. Edgar Toshiro **Yano**

Goal

- Present an architecture that helps to recognize the impacts in military operations caused by cyber-attacks, as well as present a way to identify vulnerabilities of a data network for a particular military mission. Finally, this architecture can also be used as a combat support tool for military planning.

Agenda

- **Introduction**
- **Related Work**
- **Functionalities of the Architecture**
  - **- Identification of Vulnerabilities**
  - **– Identification of Impacts of a Cyber Attack**
  - **– Mission Planning**
- **Assessment**
- **Final Remarks**

Introduction 1/4

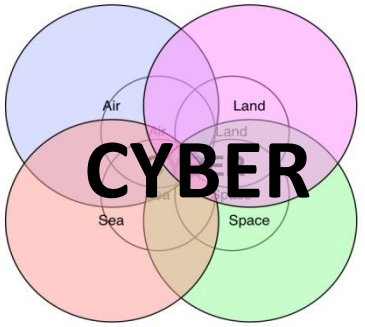
- With the growing capability of technological means and, consequently, increasing the speed of military operations, information on the battlefield has become valuable.

Introduction 2/4

- Situational Awareness (SA) of modern combat aims to meet the needs of the Command and Control (C2). In order to lead their military organizations, the commander would require concise information about his and the enemy troops.

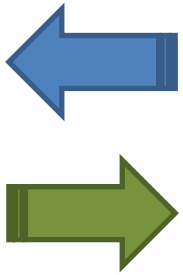
Introduction 3/4

- The information should also be timely, because important information, that is late, loses its value. This way the agility of C2, in a Military Command Center, influences directly the power combat of a military organization.
- In this context, the study of cybernetics is extremely relevant.



Introduction 4/4

- For this reason, a military commander must know the **kinetic (tactical)** and **cybernetic** battlefields. Obtaining Situational Awareness of Cyberspace can produce significant results to **tactical** actions.

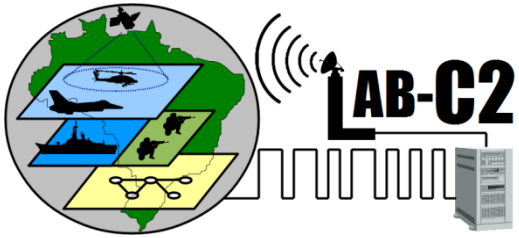


kinetic (tactical)

Cybernetic

Agenda

- Introduction
- **Related Work**
- **Functionalities of the Architecture**
  - **Identification of Vulnerabilities**
  - **Identification of Impacts of a Cyber Attack**
  - **Mission Planning**
- **Assessment**
- **Final Remarks**



18th ICCRTS

Architecture for Cyber Defense Simulator in Military Applications

Authors:

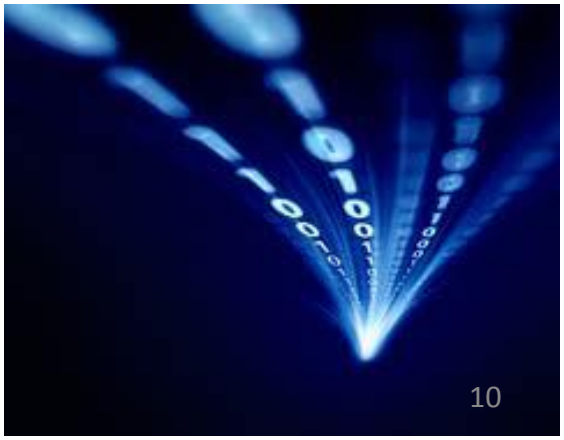
Maj André Ferreira Alves Machado

Maj Alexandre B. **Barreto**

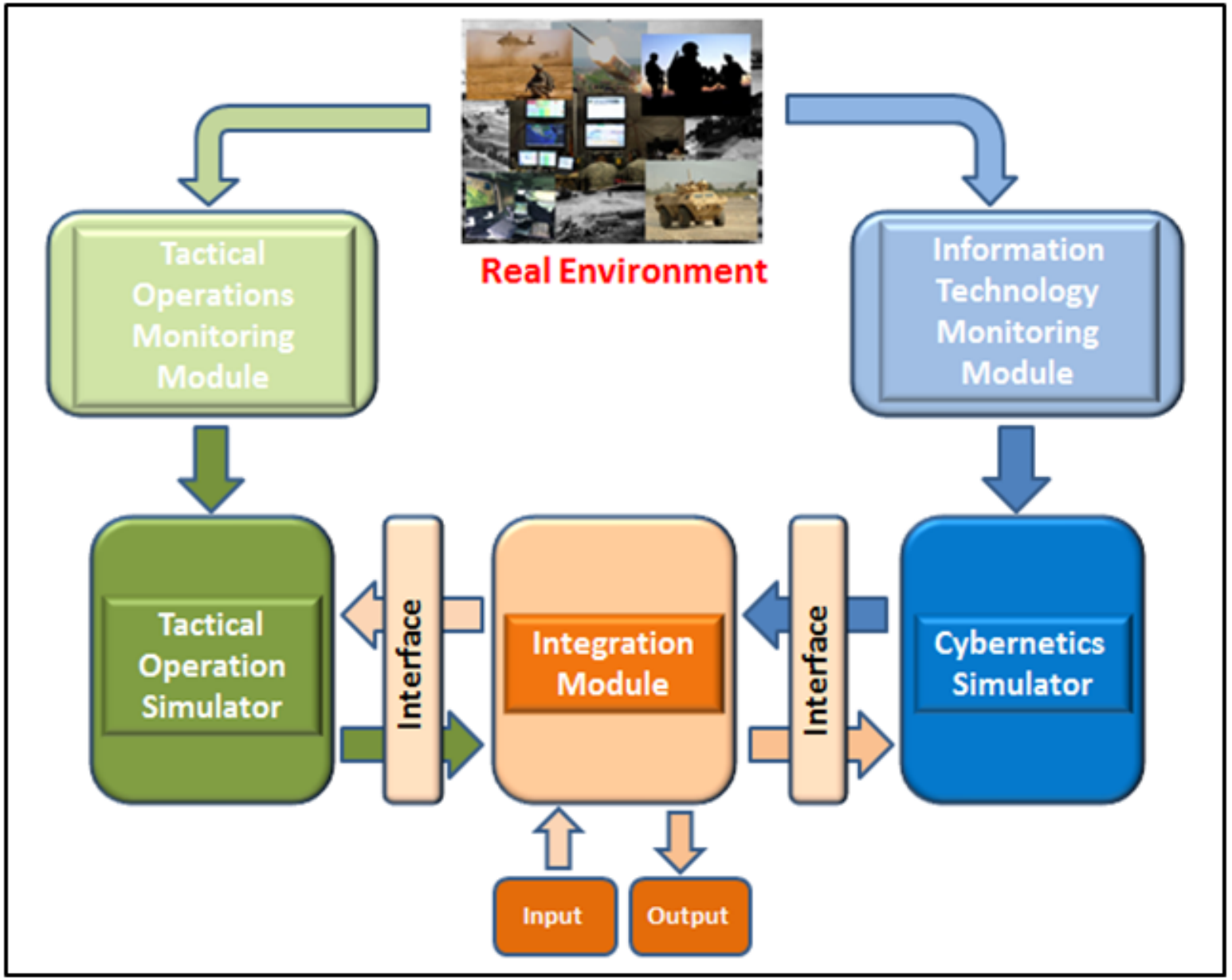
Prof. Edgar Toshiro **Yano**

Any tactical event occurs only when we have an order or make a request.

So, we need a flow of information.



Architecture (overview)



✓ Tactical actions

✓ Network topology

✓ IT assets

Real Environment

TOp

ITM2

DENIED

TOp Sim

IM

CyberSim

Output

Main goal of the Architecture

Identify which vulnerabilities we have in our network.

Agenda

- Introduction
- Related Work
- **Functionalities of the Architecture**
  - **- Identification of Vulnerabilities**
  - **– Identification of Impacts of a Cyber Attack**
  - **– Mission Planning**
- **Assessment**
- **Final Remarks**

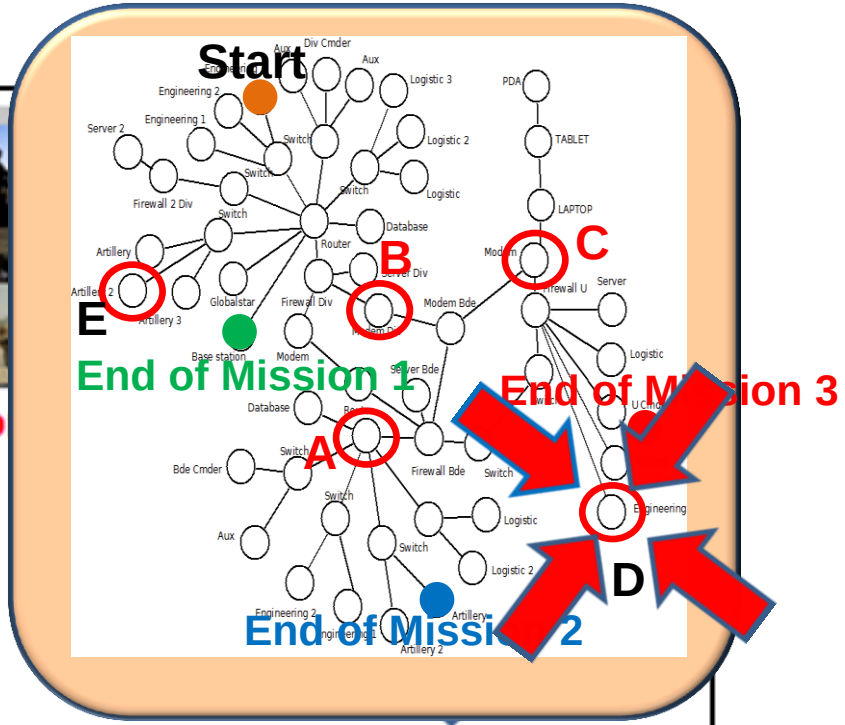
Identification of Vulnerabilities

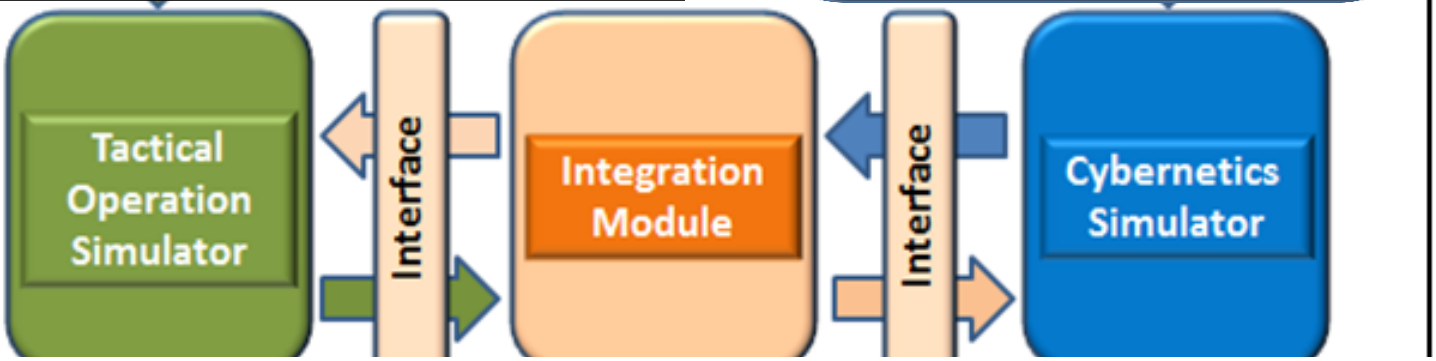
- According to some references [10, 11, 12, 13], some cyber simulators already have the functionality to identify vulnerabilities of IT assets in a data network. But, in a large data network, or in a highly dynamic network, there may be from ten to hundreds of vulnerabilities.
- In such cases, will we have time and resources to solve all the problems, without damaging the progress of a military mission?

Identification of Vulnerabilities

- In complex data networks, we need to identify which vulnerable assets can disrupt the progress of important military tasks.
- **So, we need to Identify vulnerabilities in relation to the military mission.**

Identification of Vulnerabilities in Relation to Mission





Mission	Type	Mission Status	Cyber Vulnerabilities
1	Attack order	Safe	-
2	Artillery Support	Unsafe	Assets A and B
3	Move order	Unsafe	Assets B and C

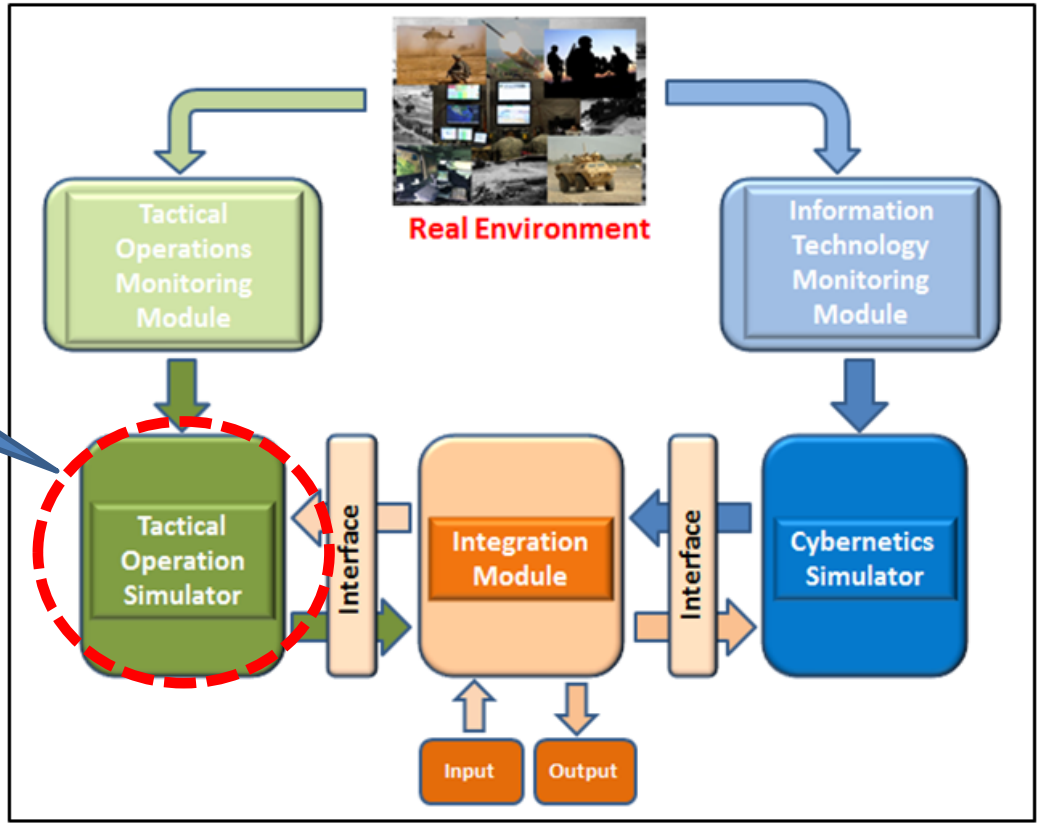
Agenda

- Introduction
- Related Work
- **Functionalities of the Architecture**
  - Identification of Vulnerabilities
  - **Identification of Impacts of a Cyber Attack**
  - **Mission Planning**
- **Assessment**
- **Final Remarks**

How are the impacts identified?

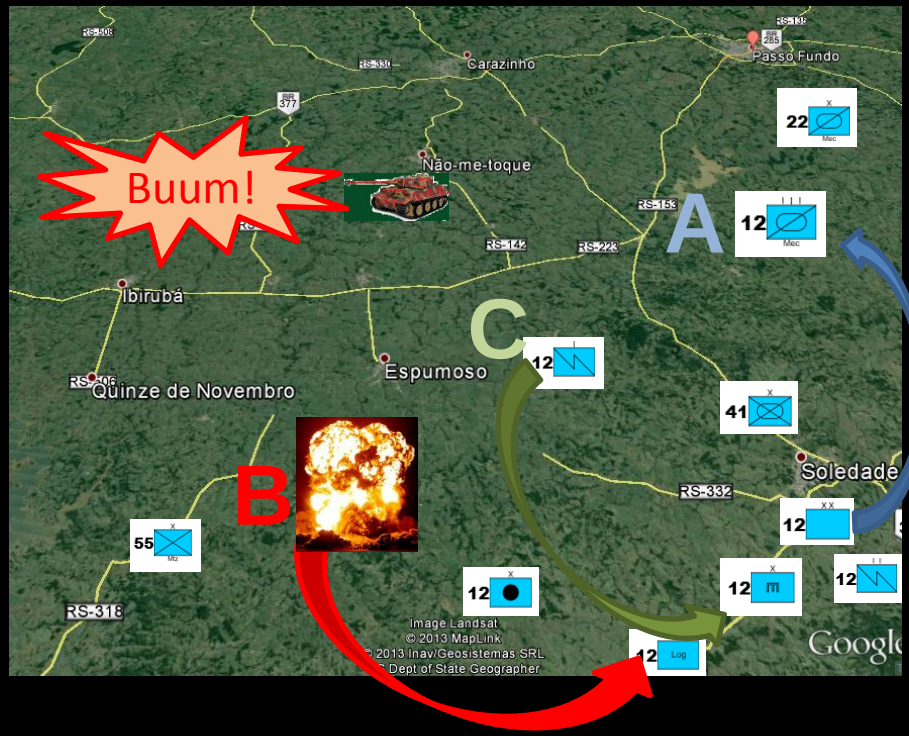
- Using the power of the simulator.

Comparing two different simulations (with and without cyber attack).



TATICO OPERACIONAL SIMULATOR (TOpSim) (According to Table 3)

With Cyber attack



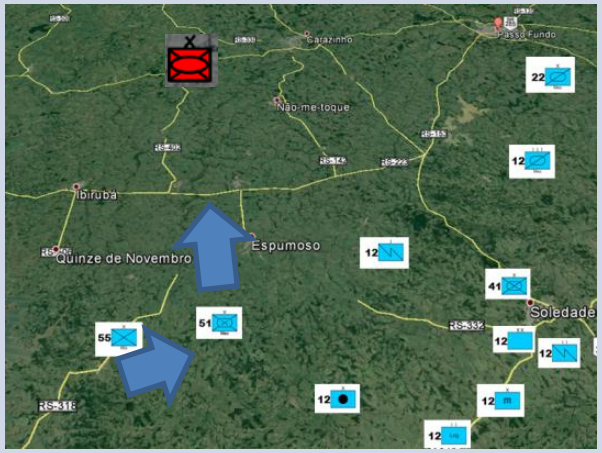
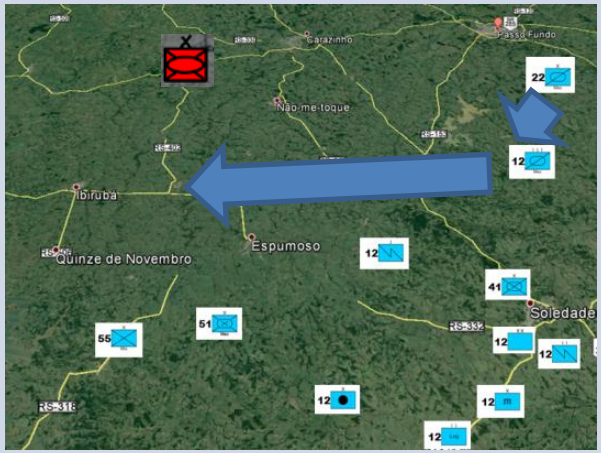
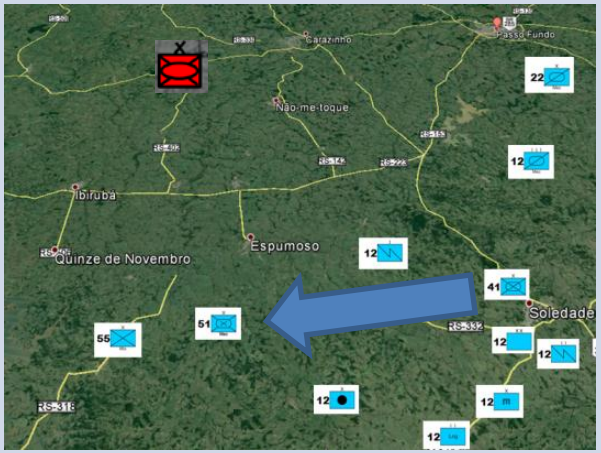
Without Cyber attack

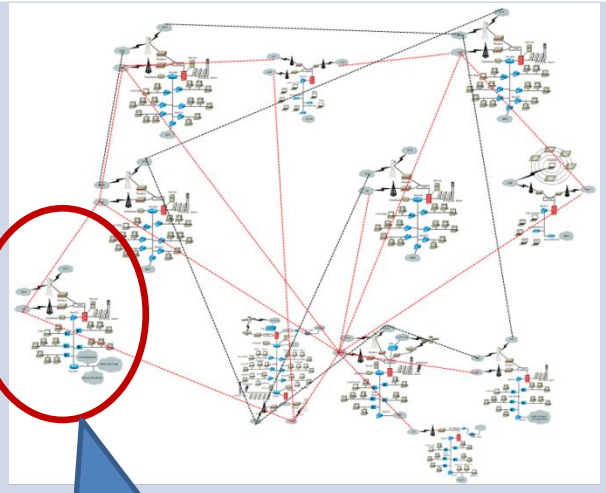
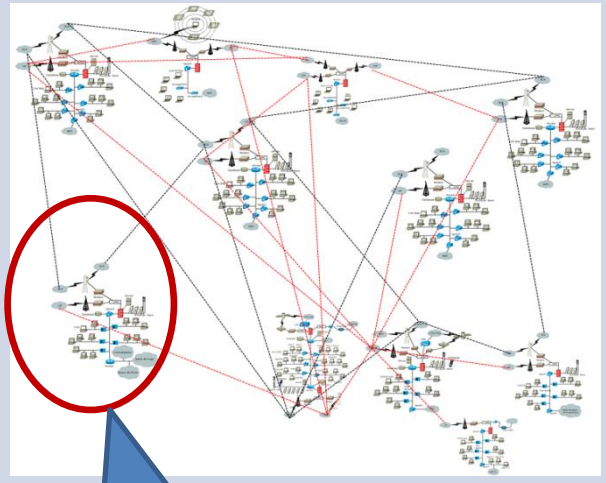
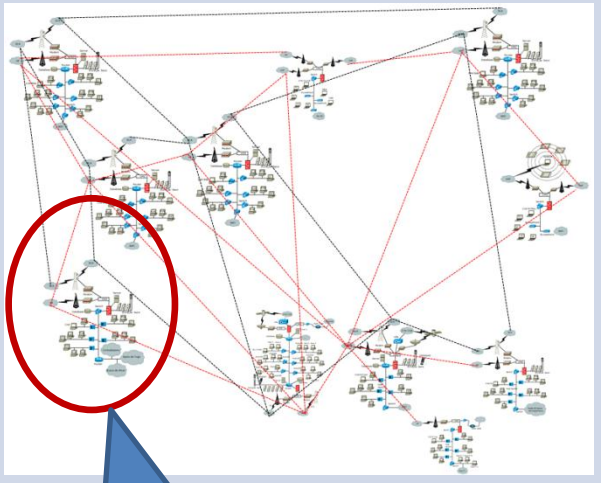
Agenda

- Introduction
- Related Work
- **Functionalities of the Architecture**
  - Identification of Vulnerabilities
  - Identification of Impacts of a Cyber Attack
  - **Mission Planning**
- **Assessment**
- **Final Remarks**

Mission Planning

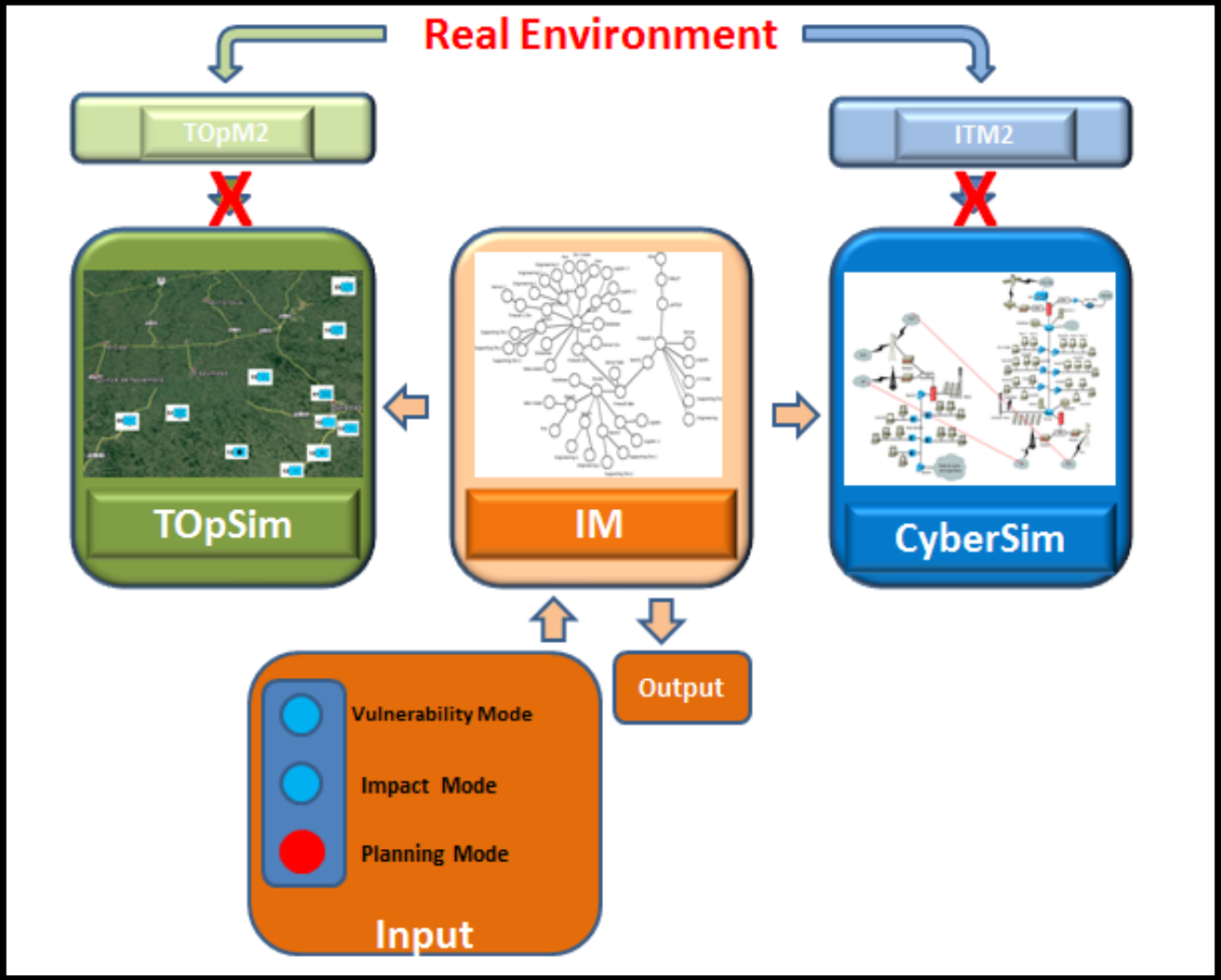
- In planning a military mission, many decisions can be made. In this study, we focus on the movement of military troops (positioning of Units on the battlefield).
- For our approach we focus on the data network that supports military actions. When we change the position of a military Unit, we are indirectly changing the topology of the data network.

Planning Alpha	Planning Beta	Planning Gamma
		

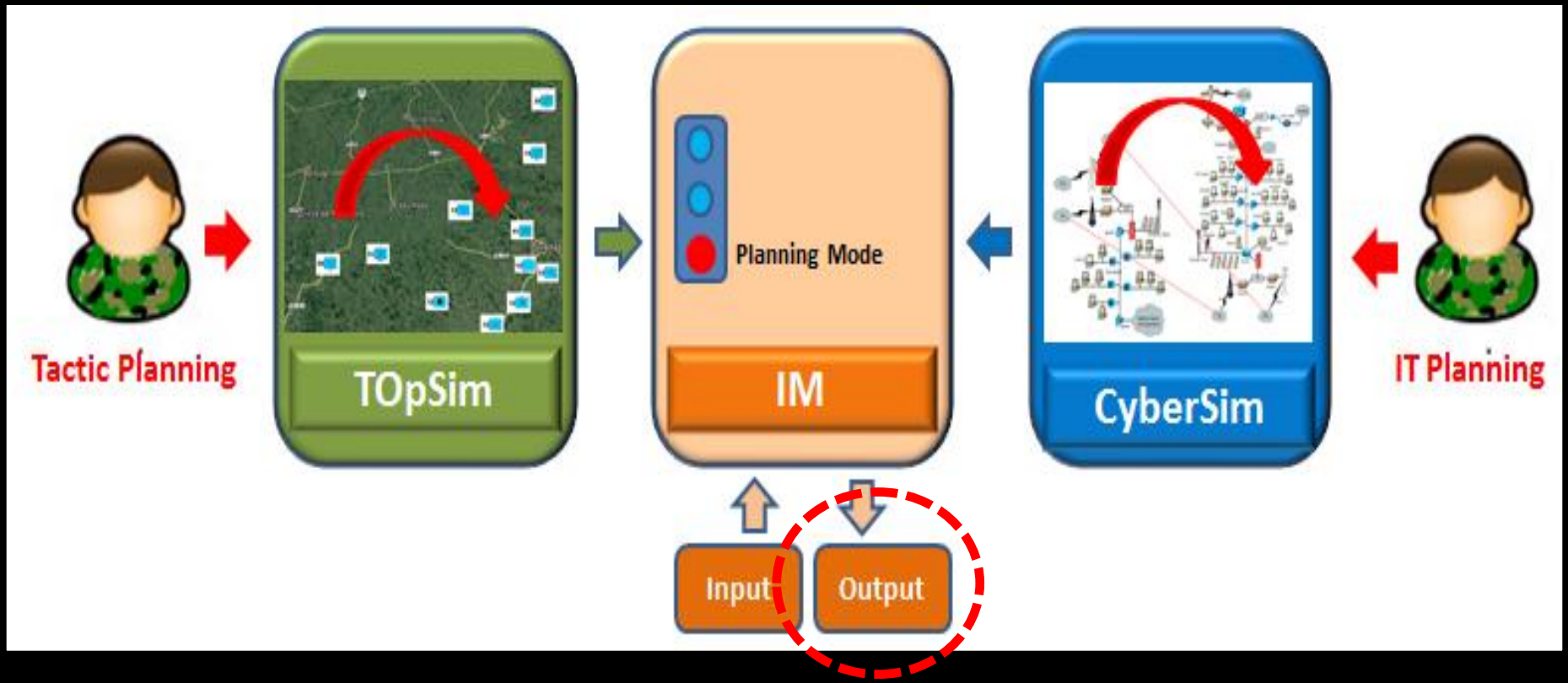
Planning Alpha	Planning Beta	Planning Gamma
		
2 links	3 links	5 links

- These changes in connections can include or exclude a set of assets in a data network. According to [6], when new assets are added or removed from a network, the network vulnerabilities also change.

Mission Planning



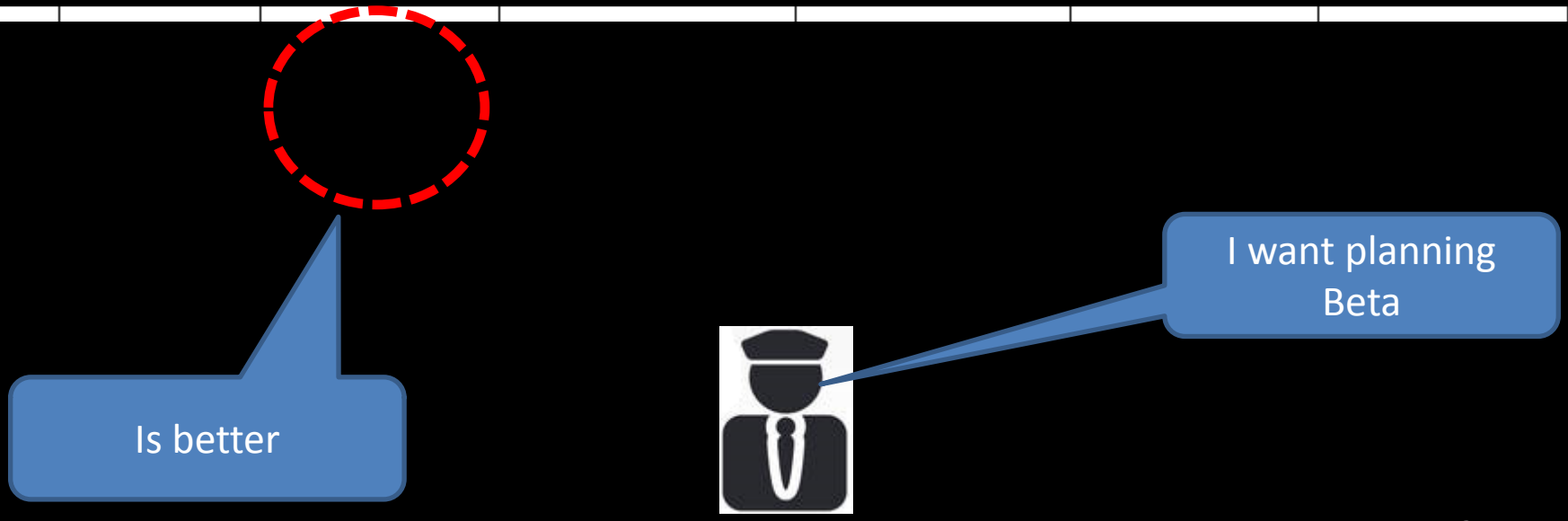
Mission Planning



Mission Planning

Table 4 – Plan Report [8]

Mission	Priority	Planning	Vulnerabilities		Risk	
			Before the planning	After planning	Before the planning	After planning



Agenda

- Introduction
- Related Work
- Functionalities of the Architecture
  - Identification of Vulnerabilities
  - Identification of Impacts of a Cyber Attack
  - Mission Planning
- **Assessment**
- **Final Remarks**

Assessment

- The proposed architecture was not implemented by the time of this paper submission. However, some simulations were done for conceptual assessment of the main module of the architecture (Integration Module).
- For the integration of the environments, IM uses the graph structure to represent real world environment (kinetic and cyber).

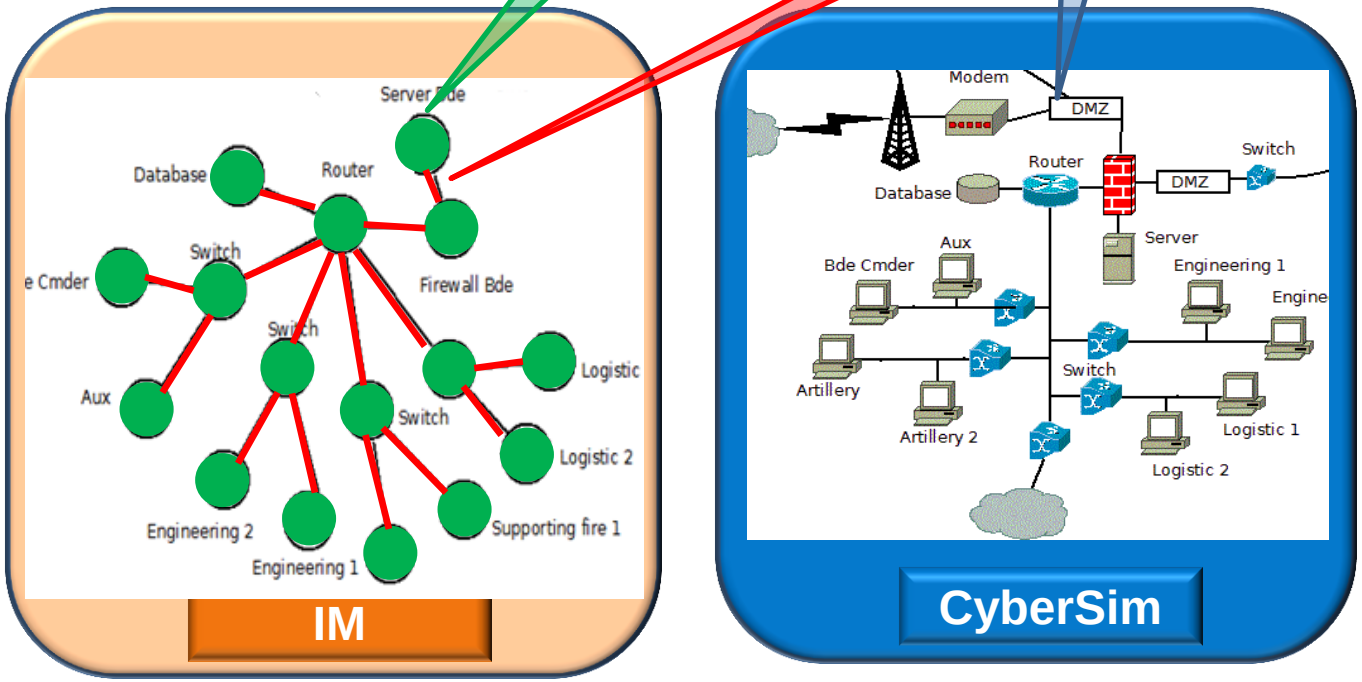
Assessment

- Therefore, we propose the use of Java Universal Network Graph (JUNG) for necessary implementation (construction and analysis of graphs) of the IM. Which in turn will help us to realize the evaluation of the approach.

Assessment (Step 1)

Construction of the Graph

- Admitting that the CyberSim has 405 assets, the graph will have at least 405 nodes and 500 edges.
- To build this graph, the algorithm needed **49ms.**

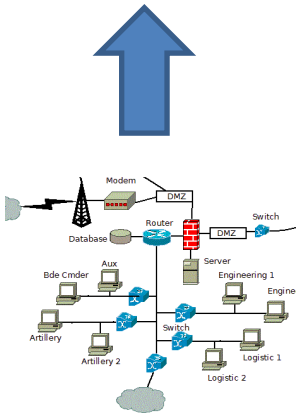


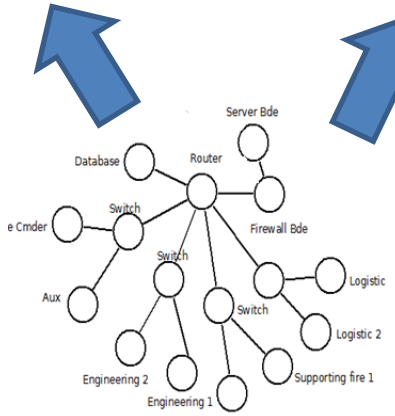
Assessment (Step 1)

Construction of the Graph

Table: Different size Graphs x time to build

Estimated Assets	Graph Nodes	Graph Edges	Average Time
1,620	1,620	2,000	79.8 ms
4,050	4,050	5,000	90.1 ms
40,500	40,500	50,000	1,570 ms
65,000	65,000	80,000	3,575 ms





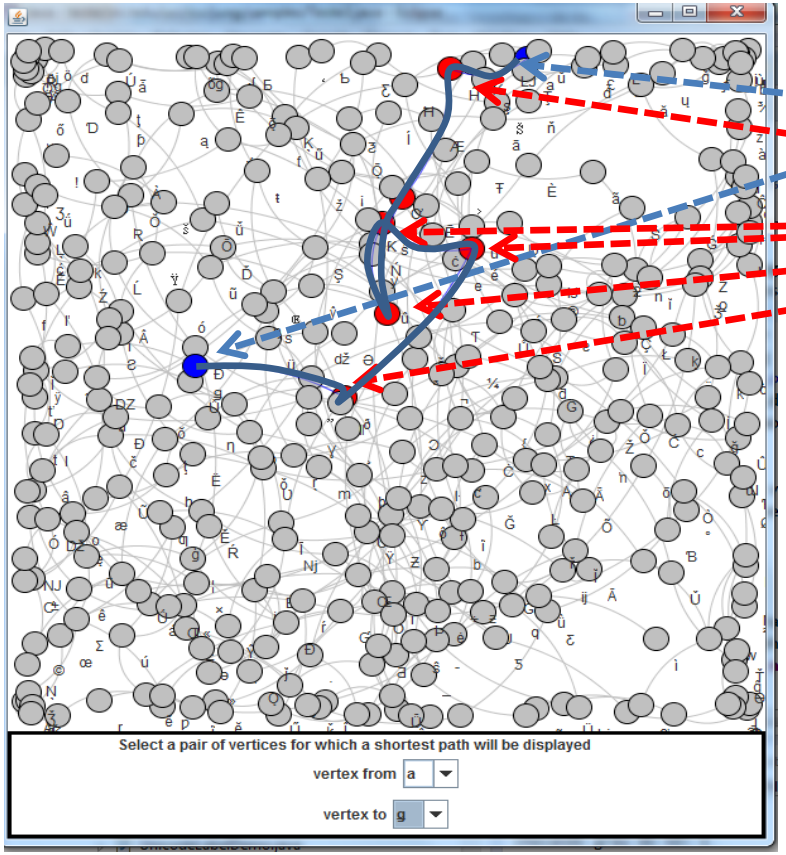
Assessment (Step 2)

Analysis of Paths in Graph

Continuing with the assessment of IM, we highlight the important requirements to verify the existence of "paths" between two nodes of the graph. For this activity, we can use *DijkstraShortestPath* algorithm.

Assessment (Step 2)

Analysis of Paths in Graph



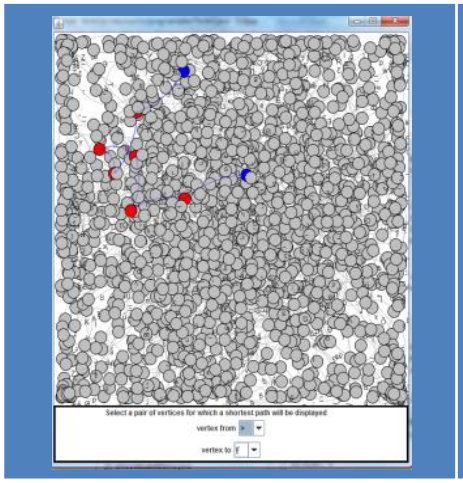
The **blue nodes** are the "start" and the "end" nodes of the path, the intermediate nodes (of the path) are **red**, and the **blue edges** are the paths taken by the algorithm.

To generate this path in a graph with 405 nodes, the algorithm took an average of **1.83 ms**.

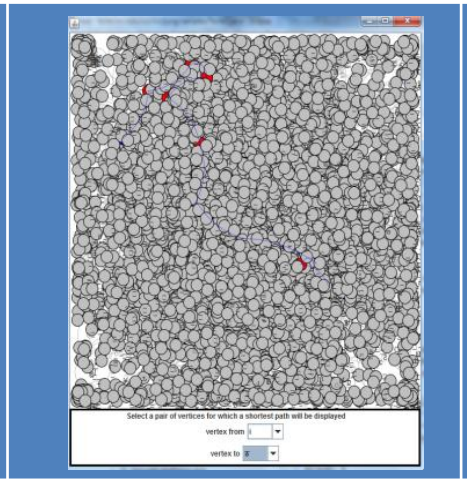
Assessment (Step 2)

Analysis of Paths in Graph

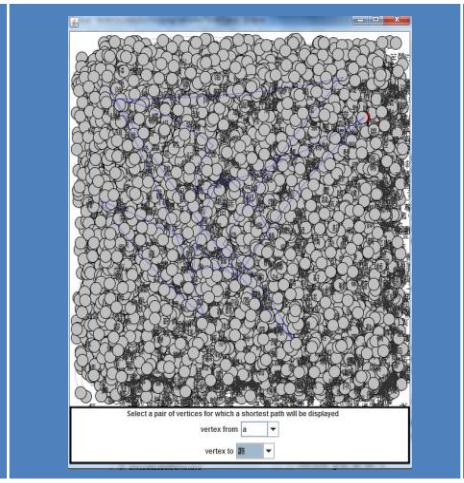
Estimated Assets	Graph Nodes	Graph Edges	Average Time
1,620	1,620	2,000	4.77 ms
4,050	4,050	5,000	12 ms
40,500	40,500	50,000	221.5 ms
65,000	65,000	80,000	229.25 ms



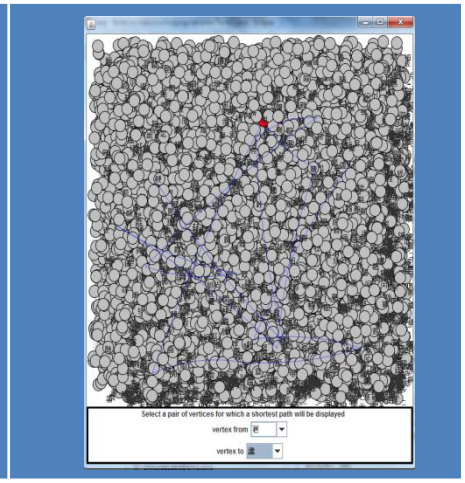
1,620 nodes



4,050 nodes



40,500 nodes



65,000 nodes

Agenda

- Introduction
- Related Work
- Functionalities of the Architecture
  - Identification of Vulnerabilities
  - Identification of Impacts of a Cyber Attack
  - Mission Planning
- Assessment
- **Final Remarks**

Final Remarks 1/3

- The main purpose of this article is to extend conceptual understanding about the approach developed in our previous article [7].
- With this goal, in this article, we present the functionalities expected for Architecture. They are: identify the vulnerabilities of IT assets, in relation to tactical missions; identify the impacts of a cyber-attack in the kinetic environment; and achieve a tactical, cyber and combined planning.

Final Remarks 2/3

- The approach focuses only on the terrestrial military environment and Denial of Service in cybernetic environment. The undocumented attacks will not be identified by the proposed Architecture.
- The assessment was not to identify a tool or an ideal programming language to perform the analyzes in graph, but rather to verify the viability (in terms of processing speed) of the use of graph theory for IM.

Final Remarks 3/3

- As future work, we propose to implement other components of the proposed Architecture; and other types of cyber-attacks, such as: interception actions, degradation and production of false data.
- Concluding this work, we believe that Architecture can also be used in other areas.

Acknowledgment

- I would like to thank the Aeronautic Technology Institute (ITA), the Technology Science Department (DCT), the Center for Integrated Electronic Warfare (CIGE) and the Brazilian Army .

References

- [1] BARFORD, P; DACIER, M.; DIETTERICH, T. G.; FREDRIKSON, M.; GIFFIN, J.; JAJODIA, S.; JHA, S.; LI, J.; LIU, P.; NING, P.; SONG, D.; STRATER, L.; SWARUP, V.; TADDA, G.; WANG, C.; YEN, J. Advances in Information Security. **Cyber situational awareness**: issues and research. New York: Springer, 2009. (Advances in Information Security, v. 46) ISBN 978-1-4419-0139-2.
- [2] DENNING, D. E. An intrusion-detection model. **IEEE Transactions on Software Engineering,** v.13, p. 222-232, 1987.
- [3] BASS, T. **Multi sensor data fusion for next generation distributed intrusion detection systems.** IRIS National Symposium on Sensor and Data Fusion. [S.l.: s.n.]. 1999.
- [4] SCHNEIER, B. (1999). Attack trees: Modeling security threats. Dr. Dobb's journal. Available: https://www.schneier.com/paper-attacktrees-ddj-ft.html. Accessed: 11 out. 2013.
- [5] MUSMAN, S.; TEMIN, A.; TANNER, M.; FOX, D.; PRIDEMORE, B. (2010). Evaluating the Impact of Cyber Attacks on Missions. MITRE Corp, McLean, VA, 22102.
- [6] JAJODIA, S.; NOEL, S. Topological vulnerability analysis. In: JAJODIA, S. et al. **Cyber situational awareness**: issues and research. New York: Springer, 2010. p. 139-153. (Advances in Information Security, v. 46)

References

- [7] MACHADO, A; BARRETO, A; YANO, E. Architecture for cyber defense simulator in military applications. In: INTERNATIONAL COMMAND AND CONTROL RESEARCH AND TECHNOLOGY SYMPOSIUM, 18., 2013, Alexandria. **Proceedings...** Alexandria: CCRP, 2013.
- [8] MACHADO, A. F. A.; YANO, E. T. Architectural concept of a simulator for cyber situational awareness. 2013. Thesis (Master degree in computer engineering). Instituto Tecnológico de Aeronáutica. São José dos Campos, 2013.
- [9] ALBERTS, D. S.; HAYES, R. E. **Understanding command and control**. Washington, D.C.: CCRP Publication Series, 2006. 255 p. ISBN 1-893723-17-8.
- [10] SKYBOX SECURITY. Developer´s Guide. Skybox View. Manual.Version 11. 2010.
- [11] SCALABLE Network. EXata communications simulation platform. Available: <http://www.scalable-networks.com>. Accessed: 16 jun. 2012.
- [12] DECATRON. **Executive project**. Cyberwar operation simulator. Rio de Janeiro. Nov. 2011.
- [13] LEEUWEN, V. et al. Cyber Security Analysis Testbed: combining real, emulation, and simulation. In: INTERNATIONAL CARNAHAN CONFERENCE ON SECURITY TECHNOLOGY. **Proceedings…** San Jose: IEEE, 2010.
- [14] STOREY, N. **Safety-Critical Computer Systems**. [S.l.]: Prentice-Hall, 1996.
- [15] JUNG. Java universal network graph framework. Available: http://jung.sourceforge.net/index.html. Accessed: 10 set. 2013.


Thank you
for your
attention

Conceptual Architecture for Obtaining Cyber Situational Awareness

André F. A. Machado - Major
Instituto Tecnológico de Aeronáutica
Brazil
majandre@ita.br
majafam97@gmail.com